

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

Among other things, the March 16, 2012 order of this court gave the government 30 days to undertake a reasonable effort to return data to defendants.¹ The data at issue fell outside the scope of the 27 warrants by which over 100 of the defendants' computers and other digital devices (including storage media) were seized.² After securing leave from the court,³ the government now seeks reconsideration of the court's return order.⁴

¹ See Docket No. 237 at 12. At the government's request, this deadline was extended. See Docket No. 249.

² See *id.*

³ See Docket No. 267.

⁴ See Docket No. 284.

1 In its March 16 order, the court already outlined *Tamura*, CDT and other pertinent Ninth
2 Circuit precedent, and will not do so again here. The grounds for the government's request are as
3 follows: (1) identifying non-targeted data might be difficult; (2) certain non-targeted data might be
4 useful in understanding data that is clearly targeted; and (3) disaggregating non-targeted from
5 targeted data might be unduly burdensome and expensive; (4) allowing only the defendants to keep
6 a complete copy of the seized data might deprive the government the ability to challenge
7 exculpatory non-targeted data and thus would be unfair. As evidentiary support, the government
8 offers a declaration from Alan Lee, Deputy Lab Director and Operations Manager for the Silicon
9 Valley Regional Computer Forensic Laboratory.

10 The court is not persuaded. Mr. Lee's declaration confirms that almost a year and a half
11 after presenting the warrants, the government has yet to take any meaningful steps to isolate non-
12 targeted from targeted data. Each of the grounds offered by the government either was presented
13 or could have been presented months ago, before the court issued its March 16 ruling. On this
14 procedural basis alone, the government's request is deficient.

15 More fundamentally, the government's argument proves too much. If separating non-
16 targeted data from targeted data and devices lawfully retained as criminal instrumentalities is too
17 hard here, it presumably is too hard everywhere. In what case where a storage device is seized
18 lawfully could a defendant or other subject of a search warrant ever secure return of data that the
19 government had no right to take? Just about every storage device can be searched more easily with
20 automated scripts than manually.⁵ Just about every storage device has non-targeted data that might
21 prove useful to understanding the data that was targeted.⁶ Just about every storage device has
22
23
24

25
26 ⁵ See Lee Decl. ¶¶ 5-8.
27
28 ⁶ See Lee Decl. ¶ 15.

1 deleted files in unallocated space.⁷ If the government's argument were accepted here, so that it
2 need not return even the bit of data that is clearly outside the scope of the warrant, the court thus
3 would render a nullity the government's pledge in just about every search warrant application it
4 files in this district that it will return data that it simply has no right to seize.⁸

5 The motion for reconsideration is DENIED.

6 **IT IS SO ORDERED.**

7 Dated: August 7, 2012



8 PAUL S. GREWAL
United States Magistrate Judge

25
26 ⁷ See Lee Decl. ¶ 14.

27 ⁸ Accepting the government's argument would also have the effect of shifting to the defendants the
28 entire burden and cost of identifying targeted data to permit disclosure of any targeted data among
the defendants.